

IN THE ABSTRACT

Please delete the original Abstract in its entirety, and replace the same with the following:

—Systems, methods and software that enable multiple servers to verify a password, without providing any single server, client or network attacker with the ability to validate guesses for the password off-line is disclosed. Password security is maintained in a very simple model, requiring no previously secured or server-authenticated channel between the client and any servers. Data may be protected by a small password, and no other keys, remains secret even against an enemy that compromises any, but not all, of two or more cooperating authenticating servers.—

BEST AVAILABLE COPY